

**ALBERTA**  
**OFFICE OF THE INFORMATION AND  
PRIVACY COMMISSIONER**

**P2012-ND-05**

**Manulife Financial**

March 26, 2012

(Case File #P2066)

**I. Introduction**

[1] On February 17, 2012, I received a report from Manulife Financial (“Manulife” or the “Organization”) of an incident involving the unauthorized disclosure of personal information. Based on the information reported to me, I have decided that there is a real risk of significant harm to individuals as a result of the incident, and therefore I require that Manulife notify the individuals to whom there is a real risk of significant harm.

**II. Jurisdiction**

[2] Under s. 34.1 of the *Personal Information Protection Act* (PIPA), an organization having personal information under its control must, without unreasonable delay, notify me of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

[3] Section 37.1 of PIPA authorizes me to require an organization to notify individuals to whom there is a real risk of significant harm as a result of an incident. It states:

37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure

(a) in a form and manner prescribed by the regulations, and

- (b) within a time period determined by the Commissioner.
- (2) If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).
- (3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.
- (4) The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization
  - (a) to notify individuals under subsection (1), or
  - (b) to satisfy terms and conditions under subsection (2).
- (5) An organization must comply with a requirement
  - (a) to provide additional information under subsection (4),
  - (b) to notify individuals under subsection (1), or
  - (c) to satisfy terms and conditions under subsection (2).
- (6) The Commissioner has exclusive jurisdiction to require an organization
  - (a) to provide additional information under subsection (4),
  - (b) to notify individuals under subsection (1), and
  - (c) to satisfy terms and conditions under subsection (2).
- (7) Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

[4] PIPA applies to organizations, defined in section 1(1)(i) of PIPA as follows:

1(1) (i) "organization" includes

- (i) a corporation,
- (ii) an unincorporated association,
- (iii) a trade union as defined in the *Labour Relations Code*,
- (iv) a partnership as defined in the *Partnership Act*, and
- (v) an individual acting in a commercial capacity,

but does not include an individual acting in a personal or domestic capacity;

[5] I have jurisdiction in this matter because Manulife is an “organization” as defined in section 1(1)(i) of PIPA, and the information at issue in this incident qualifies as “personal information” as defined in section 1(1)(k).

[6] In considering whether to require Manulife to notify affected individuals, I am mindful of PIPA’s purpose and legislative principles and the relevant circumstances surrounding the reported incident.

### **III. Background**

[7] On February 17, 2012, I received a written report from Manulife describing an incident involving the unauthorized disclosure of personal information.

[8] On February 27, 2012, my Office contacted Manulife to request that it provide additional information concerning the incident, in order for me to determine whether to require Manulife to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls and e-mail correspondence between February 27, 2012 and February 29, 2012.

[9] The circumstances of the incident as reported to me by the Organization are as follows:

- A service provider (the “Service Provider”) under contract with Manulife Financial prints tax slips, inserts them into envelopes, then mails them to plan sponsors (the entity who provides a group retirement plan for its employees), or to plan members (individual employees).
- On January 27, 2012, the Service Provider mailed T4As to plan sponsors and plan members.
- On February 1, 2012, Manulife was contacted by two individuals who reported receiving another individual’s T4A in the envelope containing their own T4A(s). The T4A is issued by Manulife, and reflects the pension income an individual received from a pension source. T4As include the member’s name, address,

social insurance number, pension and retirement income, policy number and member number.

- On February 2, 2012, Manulife contacted the Service Provider, to report the incident for investigation.
- On February 3, 2012, the Service Provider reported to Manulife that it had identified an error in a computer program, a “logic error” in the handling of the T4A “house-holding process”. Where a member or plan sponsor may require more than one T4A, the house-holding process is designed to assemble the required T4As into one envelope. The logic error caused incorrect insertion of a T4A for one member into an envelope containing another member’s or sponsor’s T4A(s).
- The Service Provider reported to Manulife that the logic error was caused by a code change specific to the T4A process used for Manulife’s group retirement plan T4A job. The Service Provider also advised Manulife that the code change had an unforecasted effect on how the data related to house-holding was read by the system during the process of inserting T4As into envelopes. More specifically, the first T4A of a house-holding package was moved into one separate envelope for mailing. The process then moved the remaining T4As for that package into another envelope and also picked up the next T4A in the job (which did not belong in the package) and inserted it in the envelope. The Service Provider confirmed that, despite the error, the expected number of envelopes was produced, and it was therefore not alerted to the issue by an incorrect envelope count.
- Manulife was provided with a list of individuals whose T4As were incorrectly inserted into other envelopes, plus a list of plan sponsors and plan members who received T4As intended for other addresses. The total number of affected individuals in this case is 711. Of this total, 78 affected individuals are from Alberta. The total number of T4As at issue is 32,000.
- By February 10, 2012, Manulife had been contacted by 15 individuals and plan sponsors reporting that they had received a T4A in error. These reports have been compared to the lists provided by the Service Provider to verify that the lists are correct.
- On February 10, 2012, Manulife sent versions of notification letters to those affected by the error as outlined below:
  1. Plan members and plan sponsors who received T4As in error received a letter asking that they return the T4A to Manulife in a postage paid envelope that was enclosed. Recipients who destroyed the slip were asked to call to verify this. A follow-up letter will be sent to those who did not respond.

2. Plan members whose T4A was sent to the wrong address received a letter describing the error. The letter confirmed when the error occurred, what information appeared on the T4A and what steps Manulife had taken to retrieve the T4A. A contact name and telephone number was provided for those who wished to call for additional information. Manulife also offered reimbursement to those individuals for the cost of credit monitoring for one year.
  3. Plan members who received a T4A in error and whose T4A was sent to the wrong address received a letter which combined content from letter 1 and letter 2.
  4. Plan sponsors were notified if their plan members were affected by the error and were sent copies of member correspondence.
- On February 28, 2012, Manulife reported to my Office that 14 T4As had been returned to the Organization - 4 individuals had called to report that they sent the T4As directly to the individual indicated on the T4A, 2 individuals advised the Organization that they had destroyed the T4A. Manulife also advised that it continue to receive telephone calls and T4As in the mail. The Organization plans to send out a follow-up mailing when the response to the Organization's first letter slows.
  - Manulife is in the process of finalizing two key steps with its Service Provider which will be implemented to prevent future incidents. These steps are the incorporation of a post-process "index" check. This function ensures that what is expected to be provided is in fact provided by utilizing an electronic verification of two different perspectives of the same output, therefore ensuring "Perspective A = Perspective B". If A does not equal B then an "alert" is automatically raised and further processing is halted until any difference is clarified. Also, the Service Provider will implement a "Regression Test Bed" for Manulife data. This will require establishing a test input file that is used to create a specific set of output, incorporating a complete level of sampling (including a House-Holding sample). This output will then be used to compare future test output.
  - In addition to notifying my Office about the incident, Manulife also provided notification to the Office of the Information and Privacy Commissioner of British Columbia, The Commission d'accès à l'information du Quebec and to the Office of the Privacy Commissioner of Canada.

#### **IV. Is there a real risk of significant harm to individuals as a result of the incident?**

[10] Pursuant to section 37.1 of PIPA, I have the power to require Manulife to “notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure.” In determining whether or not to require Manulife to notify individuals, I must consider whether there exists a “real risk of significant harm” to individuals as a result of the incident.

[11] In interpreting the above referenced phrase, it is clear that in order for me to require that Manulife notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to that individual as a result of the incident; moreover, that harm must be “significant” – it must be important, meaningful, and with non-trivial consequences or effects.

[12] Although Manulife reported that the type of harm that could result from the unauthorized disclosure of personal information is identity theft, it stated that the risk of identity theft is “mitigated by the fact that those who received a T4A in error are plan sponsors or plan members who have a relationship with Manulife. We know who received which specific T4As in error and we have no reason to believe these recipients will misuse the information.”

[13] In this case, the personal information at issue is of high sensitivity as it includes the name of the member, mailing address, social insurance number, pension and retirement income, policy and member numbers.

[14] This information could be used to cause significant harm to individuals, and provides comprehensive individual profiles that may be used for identity theft and/or fraud. The type of harm that could result from the unauthorized disclosure to this personal information is identity theft, which, in my view is a significant harm.

[15] In order for me to require Manulife to notify its affected individuals, however, there must also be a “real risk” of significant harm to the individual as a result of the incident. This standard does not require that significant harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. Further, there must be a cause and effect relationship between the incident and the possible harm.

[16] In deciding whether there exists a “real risk” of harm in this case, I considered the fact that Manulife notified the affected groups of individuals soon after the incident was discovered; the information reported to this Office by Manulife; and the type of information involved.

[17] I also considered Breach Notification Decision P2011-ND-015, in which a similar incident occurred. In that case, T4 and Relevé (tax reporting statements for Quebec residents) were inadvertently mailed to other employees in error. The organization

maintained that the risk of identity theft was low as the three affected employees were part of the same co-worker group at one location and if any information was wrongfully used there was a high probability it would be discovered. The former Commissioner did not agree with the organization that since the unauthorized disclosure affected employees of the same worker group that the risk of identity theft was lessened. He stated that “given the sensitivity of the personal information of the employees,” there was a real risk of significant harm to those individuals whose tax statements were mailed to individuals who were not authorized to receive the information.

[18] Although Manulife believes that plan sponsors and members will not misuse this information at issue in this case, the fact remains that the information is highly sensitive information in the possession of 711 individuals, the majority of whom have not returned the T4As received in error or confirmed destruction of the information. Manulife’s relationship with the plan sponsors and members may minimize the risk of financial harm to individuals; however, in my view it would be difficult to prevent the risk of identity theft from occurring, and given the large number of recipients of the misdirected T4As, to then positively determine culpability in the event of an incident.

[19] Given the information reported by Manulife, I have decided that there is a real risk of significant harm to the individuals as a result of this incident. I have based my decision on the following factors: the information at issue is of high sensitivity and could be used to commit identity theft; and, even though the individuals that received the personal information in error are known to Manulife, these individuals have access to the personal information and a significant portion of T4As have not been returned or destroyed.

## **V. Decision**

[20] Based on the information reported to me by Manulife, I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require Manulife to notify affected individuals. I understand Manulife has already notified the individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* by way of letter sent on February 10, 2012, therefore I will not require Manulife to notify again.

Jill Clayton  
Information and Privacy Commissioner